Overleigh St Mary's CE Primary School

Records Management Policy

Date policy last reviewed: Autumn 2023

Signed by:

Nov 2023

Headteacher Date:

Nov 2023

Chair of governors Date:

Statement of intent

Overleigh St Mary's CE Primary School is committed to maintaining the confidentiality of its information and ensuring that all records within the school are only accessible to 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 to meet the school's statutory requirements.

This document complies with the requirements set out in the 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 (2018) 'Data protection: a toolkit for schools'
- DfE (2018) 'Careers guidance and access for education and training providers'

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

- Data Protection Policy
- Freedom of Information Policy
- Data and E-Security Breach Prevention and Management Plan
- Disposal of Records Log
- Information Asset Register
- Archived Files Log
- IT Policy

2. Responsibilities

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

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

2.3. The DPO is responsible for the management of records at the 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 headteacher.

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 they are responsible for (including emails) 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 achievements.

3.2. **Pupils records are only stored electronically on our SIMs system and include:**

- Any preferred names
- 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 people with parental responsibility, including their home address(es) and telephone number(s)
- Any other agency involvement, e.g. speech and language therapist
- Reference to any other linked files

3.3. The following information for pupils are stored electronically on their SIM's record, on in Staff Share or Cpoms and will be easily accessible:

- Admissions form
- Details of any SEND
- If the pupil has attended an early years setting, the record of transfer
- Data collection or data checking form

- Annual written reports to parents
- Notes relating to major incidents and accidents involving the pupil
- Any information about an 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
- 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
- Examination results – pupil copy
- SATs results
- Attendance registers and information
- Absence notes and correspondence
- Parental and, where appropriate, pupil consent forms for educational visits, photographs and videos, etc.
- Accident forms – forms about major accidents will be recorded on the pupil record – on the CWAC Prime system held in Bursars office.
- Consent to administer medication and administration records
- Copies of pupil birth certificates, passports etc.

3.4. Hard copies of disclosures and reports relating to child protection are stored on our electronic CPOMs system.

3.5. Hard copies of complaints made by parents or pupils are stored electronically.

3.6. Actual copies of accident and incident information are stored separately on the school's management information system and held in line with the retention periods outlined in this policy – a note indicating this is marked on the pupil's file. 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 DPO 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 emails

4.1. Group email addresses will have an assigned member of staff who takes responsibility for managing the account and ensuring the correct disposal of all sent and received emails.

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

4.3. 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 12 months.

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

4.5. The school's expectations of staff members in relation to their overall conduct when sending and receiving emails is addressed in the school's E-safety Policy.

4.6. All emails will be automatically deleted after 12 months, unless stated otherwise.

4.7. Correspondence created by the SLT and other members of staff with administrative responsibilities will be retained for 12 months before being reviewed and, if necessary, securely disposed of.

4.8. 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.

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

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

4.11. 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.

4.12. 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.

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

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

4.15. 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.

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

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

4.18. 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.

4.19. 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.

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

Retention of Documents – The school has adopted the **IRMS Retention Guidelines** document and disposal of all documents will follow this structure. The document if held by the DPO and school office.

5. Identifying information

5.1. 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 for individuals to exercise this right.

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

5.3. 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.

5.4. 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.

6. Storing and protecting information

6.1. 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.

6.2. The IT Technician in conjunction with the DPO will conduct a back-up of information on a termly 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.

6.3. Backed-up information will be stored using a central back-up cloud service operated by the LA. The IT Technician/DPO will ensure that the location of the cloud storage and the security offered is appropriate for the information and records stored on it.

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

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

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

6.7. 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.

6.8. 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.

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

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

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

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

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

6.14. 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.

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

6.16. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients. Usually all emails are sent via Parentmail.

6.17. 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.

6.18. 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.

6.19. A record will be kept of any document that is taken off the school premises that logs the location of the document and when it is returned to the school site, this includes records that are digitally remotely accessed.

6.20. 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.

6.21. 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.

6.22. CPOMs Identifies what level of access each staff member has to data. This record details information including:

- What level of access each staff member has.
- Limits on how staff members access data.
- What actions staff members can perform.
- What level of access is changed or retained when a staff member changes role within the school.
- Who is able to authorise requests to change permissions and access.

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

6.24. 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.

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

6.26. The physical security of the school's buildings and storage systems, and access to them, is reviewed termly by the site officer 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.

6.27. All systems that allow staff and pupils to remotely access information from the school's network whilst they are not physically at the school have strong security controls in place.

6.28. The DPO decides what restrictions are necessary to prevent information or records being downloaded, transferred or printed while the user is not on the school site.

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

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

6.31. Any damage to or theft of data will be managed in accordance with the school's Security Breach Management Plan.

7. Accessing information

7.1. We are transparent with data subjects, the information we hold and how it can be accessed.

7.2. 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.

7.3. 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.

7.4. 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.

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

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

8. Information audit

8.1. 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
- Hybrid files, containing both paper and electronic information
- Knowledge

8.2. 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

8.3. The DPO (Sarah Webb) 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

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

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

8.6. An information asset owner is assigned to each asset or group of assets. They will be responsible for managing the asset appropriately, ensuring it meets the school's requirements, and for monitoring risks and opportunities.

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

9. Disposal of data

9.1. 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.

9.2. 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 DPO will keep a record of all files that have been destroyed.

9.3. Where the disposal action is indicated as reviewed before it is disposed, the DPO will review the information against its administrative value – if the information should be kept for administrative value, the DPO will keep a record of this.

9.4. 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.

9.5. Where information has been kept for administrative purposes, the DPO 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.

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

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

10. School closures and record keeping

Merger of schools

10.1. 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.

10.2. 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

10.3. 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.

10.4. 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.

10.5. 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.

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

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

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

10.9. Records will be disposed of in line with the IRMS schedule we have adopted.

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

10.11. All IT equipment will be decommissioned in accordance with the school's IT Policy.

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

11. Monitoring and review

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