Haddenham St Mary's CE School

DATA RETENTION POLICY

Date agreed by **Finance & Resources Committee**	**26th Jan 2023**
Date to be reviewed *(maximum **36** months after date above)*	**January 2026**
Date adopted by Governing Body	**7th February 2023**
Governors Committee accountable for review	**Finance & Resources Committee**
Staff member accountable for review	**Data Protection Lead**
Governor accountable for monitoring	**GDPR governor**

Rationale

The school needs to create and maintain accurate records in order for it to function. The policy for managing records at Haddenham St Mary's CE School (HSM) has been drawn up in conformity with legislation, regulations affecting schools and best practice as publicised by the Information and Records Management Society (IRMS).

Aims

The objectives of this Data Retention Policy are to ensure that Haddenham St Mary's CE School (the "School") and its governors and employees are informed about, and comply with, their obligations under the General Data Protection Regulation ("the GDPR") and other Data Protection legislation.

The School is a voluntary controlled school and is the Data Controller for all the Personal Data processed by the School.

This policy sets out guidelines for recording, managing, storing and disposing of data, whether they are held on paper or electronically in order to assist staff, and the School, to comply with the UK's General Data Protection Regulation and the Freedom of Information Act 2000 (FOIA). It should be read and used in conjunction with the following school policies and documents:

▫ Data Protection Policy

▫ Privacy Notices

▫ Data Asset Register

Members of staff are expected to manage their current record keeping systems using the Retention Policy and to take into account the different kinds of retention periods when they are creating new record keeping systems.

Benefits of the Retention Policy

There are a number of benefits which arise from the use of a complete Retention Policy:

▫ Managing records against the Retention Policy is deemed to be "normal processing" under the UK GDPR and the Freedom of Information Act 2000. Provided members of staff are managing record series using the Retention Policy they cannot be found guilty of unauthorised tampering with files once a freedom of information request or a subject access request (SAR) has been made.

▫ Members of staff can be confident about destroying information at the appropriate time and in a secure manner.

▫ Information which is subject to Freedom of Information and GDPR legislation will be available when required.

▫ The school is not maintaining and storing information unnecessarily.

Privacy notices and parental consent

Parents accept a place for their child at HSM in the knowledge that data about pupils and their parents will be collected on admission to allow for the efficient operation of the school. This data will be updated regularly and stored/ processed in order with the GDPR (2018) rules for good information handling.

Staff Induction

All new teaching and office staff will be given training on accessing and managing school records to ensure compliance with these retention time scales. As a guiding principle, GDPR requires that personal data is only retained for as long as necessary - that is, necessary for the specific lawful purpose (or purposes) it was acquired.

Any information which is held is to be kept in accordance with the Haddenham St Mary's Data Protection Policy.

Retention Periods

The IRMS 2019 toolkit retention schedule will be referred to and used. This is the basis of our retention schedule. An additional table is in appendix 1. This is for any specific data that we retain in school. These retention periods for this data are established by the school using the IRMS guidance.

Disposal of Data

When information is no longer required, it can be disposed of. For confidential, sensitive or personal information to be considered securely disposed of, it must be in a condition where it cannot either be read or reconstructed.

Skips and 'regular' waste disposal are not considered to be secure.

Paper records should be shredded using a cross-cutting shredder or placed in the secure waste bag in the school office cupboard. CDs / DVDs should be cut into pieces. Hard-copy images, AV recordings and hard disks should be dismantled and destroyed.

We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Appendix 1:

HSM data retention schedule for specific data not covered under IRMS 2019 data retention schedule or specific to our school				
Basic file description	**Data Protection Issues**	**Retention Period**	**Action at the end of the administrative life of the record**	
Children's individual assessment files with paper assessment data/tests collected at assessment points since start of time at school	Yes	1 year after children leave year 2, transferred to next school if before this time School to archive records for the year whilst children are in year 3 then securely dispose.	Secure disposal	
Child Protection files Safeguarding Chronology sheets – form part of safeguarding records	Yes	Until child leaves HSM then transfer to the new education provider Child Protection information must be copied and sent under separate cover to new school/college whilst the child is still under 18 (i.e. the information does not need to be sent to a university, for example). Where a child is removed from roll to be educated at home – or is registered as missing in education - the file should be copied to the Local Education Authority.	DO NOT DESTROY ANY RECORDS	
CPOMS – centralised system for safeguarding records	Not unless staff do not follow rules around log in procedures	School controls the data that is stored and processed on Insight. See separate GDPR privacy policy – stored in GDPR files electronically When children move school or transfer to year 3 – the records are sent electronically by secure file transfer within CPOMS.	DO NOT DESTROY ANY RECORDS	
Insight	Not unless staff do not follow rules around log in procedures	School controls the data that is stored and processed on Insight. This system syncs with SIMS. So new children are automatically added. Children who were with us in school are archived by Insight and then deleted upon request. Current year + 6 years	Retention: Until 30 days after this Agreement terminates, according to clause 15.2 and clause 15.5.3. Deletion: Customer can request total pupil deletion by contacting the Insight support team. Notes: Admin users upload pupil records from either a third-party MIS linking service, CTF, Excel	

			document, or manual direct entry via web form. They keep records up-to-date by the same process.	
Teacher/TA planner mark book	Yes	Current year +1 year	Secure disposal	
Emergency contact folder in office	Yes	Keep for current year then update annually	Secure disposal	
Pupil's exercise books	Yes	Work returned to pupil at the end of the school year. Where school is archiving and storing example books for a year then retain for 1 year and return. Must seek parental agreement.	Secure disposal if it cannot be returned	
School website - photos/content	Yes	Annual update of photos / documents	Delete files	Remove photos of any children for whom permission is retracted during the year
Staff encrypted memory sticks	Yes	Memory stick to be returned to school before staff member leaves	All files deleted and stick reset	
Staff teaching drive (P:/) Various data	Yes	Records kept in line with data period agreed Schemes of work – current year +2 years Photos – whilst children are at school, then delete after children leave Assessment data – current year and whilst children are at school – same procedure as cohort assessment folder	Delete or archive	Remove files of children that have left school or archive

Staff laptops/PCS	Yes	Staff member has a designated laptop assigned to them and network profile assigned	When staff member leaves, laptop handed back to school. School's LA Technical Support Team will erase profile and delete files. Laptops and PCs decommissioned by the School's Technical Support Team.	
Cohort assessment folders	Yes	Started at beginning of cohort's entry to school. Added to during 3 years to become a complete profile. Shred after the children have left the school or retain for trend data but personal info must be removed/children not identified	Secure disposal at end of life of records	
Class teacher assessment folder	Yes	Retain for the year then dispose. Move phonics assessments to next class teacher then file in each child's assessment folder when they leave/move school.	Secure disposal	
Class inclusion/SEN folder	Yes	Retain for the year. Pass to SENDCO at end of year- SENDCO retains records as needed under SEND data storage retention periods. Moved to SENDCO secure filing system.	Secure disposal of documents that do need to be retained.	
Tapestry	Yes	See separate Tapestry contract that ensures GDPR compliance – stored in GDPR files electronically School controls the data that is stored on Tapestry. Stored during the children's time at HSM (3 years max) then deleted.	At the end of the contract our standard practice is to delete your data from our systems after 90 days. The data will be deleted from our backup systems 90 days after it is deleted from our systems. We are happy to delete your data sooner if you ask us to.	
J2e (Just 2 Easy)	Yes	See separate GDPR privacy policy – stored in GDPR files electronically	Just2easy stores data for its users. Whilst there is an active account for a school, Just2easy will not delete any user data	

		School controls the data that is stored on J2e. Stored during the children's time at HSM (3 years max) then deleted.	without an express request from the data controller to do so. Once an account has become inactive, Just2easy will delete all data associated with that account after a period of 5 years has elapsed. At the express request of the data controller, Just2easy will delete all or any data as requested including any and all backups. Such requests should be sent via email or post.
Seesaw	Yes	See separate signed DPA and privacy notice – stored in GDPR files electronically School controls the data that is stored on Seesaw. Classes are deleted or archived after the current school year. They are archived for the time that children that are at HSM then deleted.	If you would like to delete your Seesaw account or any content submitted to Seesaw, please send an email to help@seesaw.me. If you request that your account or any content submitted to Seesaw be deleted, Seesaw may still retain information for up to 60 days to provide customer support and prevent accidental deletion.
SIMS	Yes	See separate GDPR privacy notice – stored in GDPR files electronically School controls the data that is stored and processed on SIMS.	All personal data will be held in accordance with Capita plc group policy, and historical records will not be held without legitimate reason. We have a variety of automated retention policies in place that ensure data is regularly cleared down within our system if it has not been used, updated or interacted with in a reasonable amount of time. Essentially, we will only hold your personal information on our systems for the period necessary to fulfil the purposes outlined in this privacy notice or until your request it is deleted.
RM Unify	Yes	See separate GDPR privacy policy – stored in GDPR files electronically	Today, when a user is deleted from your RM Unify establishment, we do the following: Office 365 - unlicence the user

		School controls the data that is stored and processed on RM Unify – this is a cloud based app linked to SIMS. From 2nd October 2017, we will start running a regular data housekeeping process which will spring clean your Office 365 accounts. This will remove any accounts that were linked to an RM Unify user who was deleted over nine months previously.	Tell all third party apps with auto-provisioning that the user has been deleted. This leaves you to hard delete the user from Office 365.
Microsoft Office 365 Microsoft Teams	Yes	See separate Microsoft GDPR privacy policy – stored in GDPR files electronically The school creates a Microsoft account tied to an email address, that account is known as a **work or school account** (staff and pupils). Accounts are deleted and accessed via SIMS/RM Unify. School controls the accounts and the level of access for students and staff in Teams to ensure the most appropriate level of privacy for users.	Automated retention policies in place that ensure data is regularly cleared down within our system if it has not been used, updated or interacted with in a reasonable amount of time.