"Excellence Together, Learning Through Faith"

St Mary's C of E (VA) Primary School

As a Church School we seek to ensure that the ethos and principles of Christianity underpin the experiences of the children in our care.

"St Mary's is an inclusive school where we believe that all people are of equal value, irrespective of their ethnicity, culture, religion, gender, ability or sexual identity. We recognise and respect their differences."

Data Retention Policy

This policy is GDPR compliant.

Date of issue: April 2018
Last reviewed/adopted: October 2018
Next review date: Autumn 2021

Signed:_____ Date:_____

The purpose and requirements for keeping the data

St Mary's C of E Primary School (916) is committed to the protection and security of all data it is required to keep – in some cases this may be beyond a pupil's, staff member's or governor's tenancy at the school. Considering this, St Mary's School is required to keep a Data Retention Policy pertaining to computerised data that must be kept for six or more years.

Should the school fail to retain this data, legal action may result in financial penalisation and/or negative press; it is for this reason that the school will retain relevant data for as long as it is required.

The information assets to be covered by the policy

The school understands the sensitivity of some data it is required to keep and ensures measures are in place to secure this data, in accordance with the school's **Data Protection Policy** and the GDPR.

To ensure the safety of the data and records, St Mary's School will not store any data on flash drives (memory sticks). St Mary's School understands the importance and sensitivity of some data and sees the use of flash drives as inappropriate due to the fact they can be easy to corrupt, lose or steal. Data will be stored on password protected external hard drives.

The individuals responsible for the data preservation

Data retention will be overseen by the following personnel:

- the headteacher
- Information asset owners

Should any of the above personnel change, appropriate updates will be made to this and other affected policies and correspondence.

The appropriate supported file formats for long-term preservation, and when they need to be transferred

As agreed with the **ICT coordinator**, **Microsoft Word** documents will be converted into **PDF** files, to ensure the longevity of their accessibility – file formats should be converted as soon as possible, or within six months, to ensure their compatibility. Further specifications of file conversion are listed below:

Type of file	To be converted to
Microsoft Word document	PDF
Microsoft PowerPoint document	PDF

Microsoft Excel document	PDF
Images	JPEG
Videos and film, including CCTV	MOV/MP4

The retention of all software specification information and licence information

If it is not possible for the data created by an unsupported computer system to be converted to the supported file formats, the system itself should be 'mothballed' to preserve the files it has stored. If this is the case with any data, St Mary's School will list the complete system specification for the software that has been used and any licence information which will allow the system to be retained in its entirety.

Data will be stored on password protected external hard drives, which will be kept in a locked filing cabinet – only the **information asset owners** and the **head teacher** will have knowledge of these passwords

How access to the information asset is to be managed in accordance with the GDPR

To ensure the data's relevance to the school, and that recent files have been correctly converted, Vanessa Hunt (Headteacher) and Jonathan Clarke (DPO) will undertake regular archive checks of the data – timeframes are listed in the table below. In accordance with principle five of the GDPR, personal data should be "kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed". St Mary's School is committed to ensuring all data is checked regularly to ensure its relevance.

Timeframe	Type of check
Biannually	Relevance check
Annually	Compatibility check and, if required, back-up files created
At the end of the data's lifecycle (at least every six years)	Check to ensure data is securely disposed of