St. Gregory's Catholic High School

Digital Continuity Statement

Monitoring

The implementation of the policy will be monitored by the Director of Finance and Resources.

Evaluation

The policy was reviewed by the Director of Finance and Resources and Senior Leadership Team on 24th October 2022 prior to the submission of the policy to Governors' Resources Committee for scrutiny and recommendation to the Full Governing Board for approval.

Policy Review Dates:

Date last approved by Full Governing Board: new

Date submitted to Governors' Committee: 27th October 2022

Date submitted to Full Governing Board: 7th December 2022

Review Frequency: Every 2 years

Start date for policy review: August 2024

The purpose and requirements for keeping the data

St Gregory's Catholic High School 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. In light of this, the school has developed a digital continuity statement pertaining to computerised data that needs to 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 statement

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 GDPR Data Protection Policy and the UK GDPR.

The individuals responsible for the data preservation

Data retention will be overseen by the following personnel:

- The Headteacher
- The Director of Finance
- Information asset owners
- Head of IT
- Network Manager

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 Network Manager, Microsoft Office 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' (i.e. usage of the system should be stopped, but it should be kept in good condition) to preserve the files it has stored. If this is the case with any data, the 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.

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

To ensure the data's relevance to the school, and that recent files have been correctly converted, the Head of IT will undertake regular archive checks of the data – timeframes are listed in the table below. In accordance with principle five of the UK 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". The 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