Keystone Academy Trust

Digital Continuity Statement

Created: September 2022		
Review Date: September 2023		

Signed by:

	CEO	Date:	
	Chair of trustees	Date:	

Digital continuity statement

A digital continuity statement (DCS), or data retention statement, outlines why and how Keystone Academy Trust intends to retain data that should be kept for six or more years.

The ability to properly manage digital data is essential for protecting the information that the Trust depends on to function. Correctly managed data allows the Trust to operate legally, efficiently and effectively.

Keystone Academy Trust will manage their information as an asset, ensuring that it is sourced and managed for as long as required. It is important that data remains accessible yet secure, so that it is available to use, when necessary, in the future, e.g. if legal charges are ever brought against the Trust.

Records deemed appropriate for the DCS should be identified early in their lifecycle, so the appropriate measures can be taken. Similarly, data that does not require inclusion in the DCS should also be identified early on, to avoid retaining excess data.

The purpose and requirements for keeping the data

Keystone Academy Trust 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 within the Trust. In light of this, the Trust has developed a digital continuity statement pertaining to computerised data that needs to be kept for six or more years.

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

The information assets to be covered by the statement

Keystone Academy Trust 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 Trust's Data Protection Policy and the UK GDPR.

The Trust's data security measures are outlined in full in the Data and Cyber Security Breach Prevention Management Plan.

The individuals responsible for the data preservation

Data retention will be overseen by the following personnel:

- Headteacher, Head of School, Trust Chief Finance Officer, Trust Chief Operations Manager and CEO.
- Information asset owners e.g School administrators, Deputy CFO

Should the 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

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' (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 Trust 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 Sharepoint file, – only the information asset owners and the headteacher or Head of School will have knowledge of these passwords

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

To ensure the data's relevance to the Trust, and that recent files have been correctly converted, information asset owners 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 Trust is committed to ensuring all data is checked regularly to ensure its relevance. These checks will be audited centrally at either school or trust level.

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