Fairfield School
Embracing Uniqueness

Digital Continuity Statement

Nov 2020

Version	1.0
Date Approved by Governors:	10th Nov 2020
Review date:	10th Nov 2022
Version History	

Digital continuity statement

A digital continuity statement (DCS), or data retention statement, outlines why and how a school intends to retain data that should be kept for seven or more years.

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

Schools should 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 school.

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.

Digital continuity statement

The purpose and requirements for keeping the data

Fairfield 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 members or governor's tenancy at the school. In light of this, **Fairfield School** is required to keep a digital continuity statement 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 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 **Data Protection Policy** and the GDPR.

To ensure the safety of the data and records, **Fairfield School** will not store any data on flash drives (memory sticks). **Fairfield 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:

- **Person responsible for the digital continuity strategy, e.g. the headteacher**
- **Information asset owners**

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

As agreed with the **ICT provider/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, **Fairfield School** will list the complete system specification for the software that has been used and any license 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 **headteacher** 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, **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 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". **Fairfield 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

This policy will be reviewed on a bi-annual basis.