Digital continuity statement

Every Child Every Day Academy Trust

The purpose and requirements for keeping the data

The Every Child Every Day 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 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 Data Protection Policy and the UK GDPR.

[New] The school'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
- Data Manager
- HR Manager
- GDPR Lead

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

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.

Data will be stored on password protected external hard drives, which will be kept in a locked filing cabinet – only the IT Managers and the headteacher 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 school, and that recent files have been correctly converted, **the Data Manager and IT Manager** 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.