Data Retention and Security Policy, McMillan ECC

Purpose of this Policy

The school needs to create and maintain accurate records in order for it to function. The policy for managing records at McMillan has been drawn up in conformity with legislation. This policy sets out guidelines for storing and disposing of data, whether it is held on paper or electronically, in order to assist staff, and the School, to comply with the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FIA). It should be read and used in conjunction with the following policies:

- Data Protection Policy
- Information Security Policy
- Admissions Policy and Procedure

This policy seeks to ensure that:

- Members of staff can be confident about destroying information at the appropriate time.
- Information which is subject to Freedom of Information and Data Protection legislation will be available when required.
- The school is not maintaining and storing information unnecessarily, i.e. personal data is only retained for as long as necessary - that is, necessary for the specific lawful purpose (or purposes) it was acquired.

Members of staff are expected to manage their current record keeping systems using this Policy and to take account of the different kinds of retention periods when they are creating new record keeping systems. It is important that all staff bear in mind, when creating documents and records of any sort (and particularly email), that at some point in the future those documents and records could be disclosed - whether as a result of litigation or investigation, or because of a subject access request under the DPA. The watchwords of record-keeping are therefore ***accuracy***, ***clarity***, ***professionalism*** and ***objectivity***.

Practical Measures for Retention, Storing and Disposal of Data

See "Data Map at McMillan": this documents which Data we hold, where it's kept and for how long, who has access to it, and what secure measures are required, how and when we dispose of it.
Staff access to Data is considered on a need to know basis, e.g. Child Protection data is kept by the Designated Safeguarding Lead. For confidential, sensitive or personal information to be considered securely disposed of, it must be in a condition where it cannot either be read or reconstructed. Skips and 'regular' waste disposal are not considered to be secure.
Paper records should be shredded using a cross-cutting shredder; CDs / DVDs / diskettes should be cut into pieces. Hard-copy images, AV recordings and hard disks should be dismantled and destroyed. Where third party disposal experts are used they should ideally be supervised but, in any event, under adequate contractual obligations to the school to process and dispose of the information securely.