

RECORDS MANAGEMENT POLICY

|  |  |
| --- | --- |
| **Person responsible for policy:** | Emma Shaw |
| **Date approved:** | April 2022 |
| **Review date:** | April 2025 |

# Rationale.

This policy applies to all records and personal data that are maintained by the school as the Data Controller. These records are kept in order for the school to carry out its functions. These records may be retained for a set period to provide evidence of its transactions or activities. These records may be kept in hard copy or electronically. A small percentage of the school’s records may be kept for permanent preservation as part of the archives and for historical research.

# Aims.

To provide clear guidance on the storage of records including personal data, by Park Lane School.

To provide clear guidance on the length of time individual records will be stored at Park Lane School.

# Responsibilities.

The school is the Data Controller and has a responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The persons responsible are the Head Teacher and the Data Protection Officer. The Data Protection Officer will give guidance for good records management practice and will promote compliance with this policy.

Individual staff must ensure that records for which they are responsible, are accurate and are

maintained and disposed of in accordance with the school’s records management policy.

# Recording Systems.

It is important that files are reviewed regularly, at least annually, and extraneous information is removed. Removing of information once a Freedom of Access request has been made will be a criminal offence.

Once a file has been closed it should be stored in the archive store in school or in an appropriate place on the school server until the end of the retention period.

Information security is very important especially when dealing with personal data. There are a number of rules:

* All personal data should be stored in lockable filing cabinets which are kept locked when the room is unattended or on the server to which access is password protected.
* Personal data held on computer systems should be adequately password protected.
* Where possible personal data should not be sent by email.
* If files need to be removed from the premises they should be secured in the boot of the car and not left in the car overnight.
* Staff may carry data on memory sticks or external hard drives in order to access files at home or in school. Any data carried in this way must be encrypted using appropriate equipment.
* All computer based information should be backed up regularly and the backup should be stored off site.
* Emails containing personal data should only be sent using a professional email address. Where personal data is contained within an email it should be stored into the electronic filing system.

# The Safe Disposal of Information using the Retention Schedule.

Files should be disposed of in line with the retention schedule (See attached). This process should be undertaken on an annual basis in September.

All personal data should be shredded before disposal.

Electronic data should be archived on electronic media and deleted appropriately at the end of the retention period.

# Monitoring and Review.

This policy will be reviewed biannually