Financial and Information Security Policy

Stepping Stones Nursery School handles sensitive cardholder information on a regular basis. Sensitive Information must have adequate safeguards in place to protect the cardholder data, cardholder privacy, and to ensure compliance with various regulations, along with guarding the future of the organisation.

Stepping Stones Nursery School commits to respecting the privacy of all its customers and to protecting any customer data from outside parties. To this end management are committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.

Those handling sensitive cardholder data should ensure:

- Company and cardholder information is handled in a manner that fits with their sensitivity and classification;
- Protect sensitive cardholder information;
- Keep passwords and accounts secure;
- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended;
- Information security incidents must be reported, without delay, to the nursery duty manager.

The Nursery Owner/Managers have overall responsibility for financial and information security within the nursery.

All financial information retained by the nursery will be stored in a secure, locked cupboard either within the Manager's Office in the nursery building or in the Meeting Room at the Business Centre.

Information to be retained will include the bank details of employees and weekly and annual fee documents for clients.

The only members of staff to have access to any of this financial information will be Caroline O'Malley and Carol-Ann Lawson, the Nursery Owner/Managers.

The Depute Manager, Jordan Palmer, will have access to some information, as deemed necessary by the managers.

All nursery staff are aware of payment procedures. Card payments will be put through either by the nursery managers or by the depute manager. Cash payments are no longer accepted by the nursery.

All merchant copies of credit and debit card receipts are kept separately from any other financial information, in the Manual Payments folder, in a locked cupboard within the manager's office.

Any written record made of client's credit/debit card details will be destroyed using a crosscut shredder after the transaction has been processed. Under no circumstances will information pertaining to client's credit/debit cards be retained.

The only card processing method used is 1 Worldpay iCT250 terminal which is connected to a phoneline. The terminal is situated in the manager's office.

The company will renew its PCI DSS compliance on an annual basis.

The company will review its Financial and Information Security policy annually.

Policy reviewed	February 2019
Policy due for review (not more than 3 years)	Annually – 2020