St Luke's Church School

SECURITY POLICY

Ratified and shared with staff, parents and visitors
Thursday 16th November 2017
To be reviewed Autumn Term 2019

Purpose:

To provide a safe and secure environment for pupils, staff and visitors. The Security Policy ensures that effective procedures are in place to achieve this.

Security Strategies in School:

Staff

- Only staff based in school are to know the combination of the entrance door locks *(combination to be changed when a member of staff leaves/or at termly intervals)*

- Staff to contact the school office or senior staff member in an emergency

- Staff to have due care over their own safety during meetings with parents, ensuring a colleague is aware that a meeting is taking place

- All staff must challenge visitors who do not have identity badges

- During closure periods staff to inform key holder:
    - of any 'quick release' doors that they have opened
    - when they are leaving the building

Visitors

- Diary to be updated to ensure the office employees are aware of all visitors due to the school – this is a whole staff responsibility

- All visitors, including contractors, Local Authority etc., should enter via the main school entrance, report to the school office and sign in – visitors will be issued with an ID badge upon signing in at reception, and given a safeguarding leaflet.
  Visitors are to be advised by office staff that the badge must be worn and be clearly visible whilst on site. The badge must be returned upon signing out.

- The appropriate use of mobile phones will be communicated to all visitors/contractors and attention drawn to the schools safeguarding responsibilities.

- Any visitor or contractor without the appropriate safeguarding checks will be escorted by a DBS checked member of staff at all times.

- All staff to ensure that any visitor enters via the main school entrance and reports to the office

- Parents to be reminded of security strategies on a regular basis by information being included in newsletters and the website.

In School

- All external doors to be kept closed when rooms are vacant

- Vigilant record keeping and control to be exercised over all key holders and those with knowledge of the access and intruder alarms

- All rooms / cupboards containing equipment that may pose a risk to be kept locked

- A fire drill to be held at least once every term, ensuring that the alarm is tested and demonstrating that full evacuation of the building is achieved within an acceptable time

- All windows to be secured and lights and computers to be turned off at the end of the day by teaching staff and checked by the Site Manager. **If you 'open' or 'turn on' – 'close' or 'turn off' before leaving the room.**

- All doors to be locked and alarms set at the end of each day

Outside School

- Vehicular school gates to be locked at 8.30am until 3.30pm to ensure children and parents are able to have pedestrian access without danger from vehicles

- Visitors to park at nearby Tesco's to reduce opening of vehicle gates during the school day – footer note on headed paper to state no parking on site during term time

- Pedestrian gates will be locked from 9.00am until 2.50pm so that the only access point throughout the school day is via the main reception entrance

- All staff to challenge visitors on school grounds, when it is judged safe to do so, OR notify the school office immediately

Security of Equipment

- All expensive, portable equipment to be marked as belonging to the school

- All valuable and recognisable equipment to be photographed

- Intruder alarm system to be in operation when the school is closed

- Staff to be responsible for returning equipment to the appropriate area

- Staff to "sign-out" any equipment removed from school premises

- During PTFA/school/lettings events, all rooms not in use to be kept locked

Roles and Responsibilities

All staff are to take shared responsibility to ensure that security strategies are implemented.

The Headteacher will be responsible for implementing the Security Policy agreed by the Governing Body.

The Headteacher will ensure that:

- All staff appreciate the importance of security and understand the school's policy and their responsibilities

- Staff training needs are reviewed and training is provided as necessary

- Parents are aware of the Security Policy and encouraged to help

- Formal risk assessments are carried out

- There are risk assessments conducted by the Business Manager and Site Manager

- In addition, routine security checks are carried out by the Site Manager

- Termly reports are made to the Finance, Premises and Personnel Committee, relating to any security issues such as, breaches, break in's and theft.

- All crimes are reported to the Police

Role of the Governing Body

The Governing Body is responsible for formulating the Security Policy and monitoring its implementation.

Information Security

- Personal data is held securely at school level and access is by authorised personnel only. Where passwords are used for computerised records, these are strictly for the sole use of the individual to whom they are issued, regardless of the issuing authority. Where appropriate, passwords give access to limited areas of the school's ICT systems.

- An automatic lock-down policy is in operation, ensuring computers switch to 'saver mode' when there is no activity for ten minutes.

- Computer screens and documents are used in such a way as to ensure that any personal data on display is not visible to a casual passer-by.

- No personal data is stored on the hard drives of laptop computers. Where it is necessary to transport personal data on the hard drive of a laptop computer, this is strictly a temporary measure, pending the completion of a task.

- Any sensitive or personal printed material ready for disposal is shredded.

- Any used memory sticks etc are cleared before re-use to ensure that no personal data can fall into unauthorised hands. Any data residing on old equipment is cleared before disposal – including the hard drives of photocopiers.

- Where staff take personal data off-site, every care is taken to ensure that the data is secure. If data is copied to another computer to facilitate handling, the copy is erased when the task is complete. No such copies of personal data should remain on unattended hard drives or servers.

- Personal data is shared only with the data subject and other bodies that are registered data controllers such as the Local Authority, QCA, LSC, DCSF, Connexions and the Police.

- Disclosure of personal information over the telephone is strictly controlled and only takes place once the identity and authority of the caller is confirmed.