DSP/SJG/2015

DATA SECURITY POLICY

Rationale

The governing body considers that it is in their best interest, and those of the Principal and staff, as well as a requirement under insurance policies that effective security arrangements are followed at school.

Policy

1 The protection of the school's assets is essential and unless carefully and properly maintained will lead to unnecessary loss and could invalidate insurance policies.

2 The Principal shall be responsible for arranging proper security at all times for all buildings, stocks, stores, furniture, equipment, money etc., under the school's control.

3 The Principal shall be responsible for maintaining proper security and privacy in connection with personal information held on any computer to which the school has access.

4 The Principal is required to ensure that accounting records and supporting documentation are properly safeguarded to prevent loss, destruction or unauthorised alteration.

5 On a day to day basis, many of these functions will be carried out on a delegated basis by the business manager, ICT technicians, site agents and other responsible staff,

Guidelines

1 The Principal will liaise with the staff and Site Agents to ensure that proper security is maintained for all buildings and contents.

2 Keys to the safes will be held by named staff and will be carried by the individuals and not left on the premises at any time. The knowledge of the combination numbers to the safes in North and South School Offices will be restricted to:

- **North School – Finance Officer, Business Manager, Principal or Head of School**
- **South School – Office Manager, Business Manager, Principal or Head of School**

3 All key administrative data will be backed up daily.

4 Computer data will be backed up on a daily basis to a backup server in the Design Technology building. Reports of each backup task are monitored and stored.

5 Administrative access to the IT systems will be placed in escrow to the Head Teacher as a contingency against an emergency that prevented ICT staff being available.

6 An exercise to test the integrity of the backup data will be undertaken once per term

7 The governors and Head Teacher will register with the Data Protection Register under the Data Protection Act 1984. It will be the responsibility of the governors and Head Teacher that all procedures adhere to their register entries.

8 Access to the various packages within the SIMS administration software will be organised and monitored by the SIMS Manager. Decisions about access rights will be made by the SIMS Manager in consultation with the SLT member with responsibility for ICT where necessary.

9 Remote access to the school network will be password protected at all times.

10 All colleagues working within the school should ensure that they do not reveal access passwords to colleagues or students. Colleagues should also ensure that they do not leave computers logged on when the machines are unattended.

11 Inappropriate use of computers in ways which compromise the security of the network, or violate the rights of individuals will be viewed very seriously. Responsibility for decisions on disciplinary sanctions for students who abuse the computer network will rest with the member of SLT with ICT responsibility. Responsibility for investigating allegations of staff abuse of the network will rest with the Principal. Any sanctions which involve restrictions on network access will be implemented and monitored by the ICT technician team.

12 Students and their parents will be required to sign a declaration when they join the school agreeing to be bound by the terms of the school policy.

Intended Outcomes

1 A secure building and contents.

2 Secure financial and administrative data.

3 An ability to recover financial and other administrative data in the event of computers going down.

4 Adherence to the Data Protection Act.

5 Financial documents held securely.

Monitoring, Evaluation and Review

The system will be monitored and evaluated by the Senior Leadership Team and reviewed every three years by the Governors' Finance Sub-Committee.

Dissemination of the Policy

The policy will be circulated to all members of the Senior Consultative Group, relevant office staff, Computer Administration Manager and available on request to parents, the LA and OFSTED through the Principal.

Other policies that have relevance to Data Security:

School Security
Charges and Remission
ICT acceptable use policy

Date approved by the governing body	March 2015
Date to be reviewed	March 2018