Data Protection and Confidentiality Statement

Staff and Trustees

I confirm that I have read the Data Protection Policy and adhere to the clauses within them with regard to confidentiality and data protection.

For the purposes of this document, 'Personal Data' includes all personal and sensitive data for children and staff.

I undertake to follow the procedures below to ensure that personal data is secure:

- All personal data held must be accurate, relevant and secure.
- Explicit consent must be sought for collecting and sharing data for purposes other than for a legal basis, such as using photographs or completing surveys (Admin retain all student consent forms).
- Documents which hold personal data will be kept secure.
- If documents are removed from the school for an approved purpose, they will be carried safeguarded at all time (paper files) or on an encrypted data stick (electronic). The Headteacher's approval is required prior to the removal of personal data from the school.
- Passwords will be kept confidential, secure and changed as per network policy.
- Any loss or potential loss of data or breaches of confidentiality must be reported immediately to the Data Protection Officer (DPO).
- For the purposes of taking books home for marking, books must be kept securely during transportation (public transport must not be used). Children will be advised not to use photographs on their books.
- Passwords for the computer system and (SIMS) must not be on display or easily found on desks, if you write down passwords they must be kept locked away at all times.
- Computers must be locked or shut down when leaving the room.
- Online tools or systems that require the use of personal data (student/staff) are not to be used without consultation with the Headteacher.
- School personal data will not be held on personal computers at home.
- All staff will ensure that they possess no personal data on home computers, non-encrypted data sticks, hard drives or in paper form.
- Emails containing personal data will only be sent when there is no other option and only to other e-mail addresses known to be secure and accessed only by the intended recipient.
- Minutes of meetings should use initials and not full names.

Name: …… Signed: …… Date: ……

Examples of Data Breaches include, but are not limited to the following, and are potential disciplinary breaches:

- *Sending e-mails / letters to the wrong address.*
- *Leaving files containing confidential information in a public place.*
- *Staff removing information from school which they are not permitted to.*
- *Failing to keep personal details of separated parents confidential.*
- *Sending confidential information by unsecured post which goes missing.*