St Luke's CE Primary, Endon
General Data Protection Regulations (GDPR)
Staff Code of Conduct
(in conjunction with General Code of Conduct & Appropriate Use Policy)

All staff are responsible for ensuring that data used by our school is kept secure, used only for the purpose it is collected, is accessible to the Data Protection Officer (DPO) as required and can be destroyed safely after an appropriate period.

The staff code of conduct seeks to ensure that we are GDPR compliant as an organisation, and protects individual staff members and the organisation should a data breach occur. Hope Kirkham is the school Data Protection Officer (employed by SUAT on behalf of the Trust and its associate schools.

The following guidelines should be upheld at all time in order to support compliance:

1. Pupil names used in any documents or correspondence (including emails) other than official application/medical/SEN forms (where parental permission has been previously agreed) should be pseudonymised. This should be done using pupil initials eg. Ryan Giggs would be RG – this is intended to ensure that nobody beyond the employees of this organisation, or requisite external agencies, can identify the individual in question.

2. When using systems that can be accessed from home to support planning i.e. DCPro - pupil data should not be downloaded onto personal devices. If staff work away from school, data should only be saved to an encrypted/password protected school device, encrypted memory stick or emailed to your work email address.

3. All work related emails should only be delivered and received through the school email system. The school email system should not be used for personal emails.

   Any emails received from parents of pupils regarding incidents/concerns related to their child should be transferred to the appropriate correspondence file on the school server and then deleted from emails. These should not be part of a thread, as parents will have been invited in to discuss the content of their email and a meeting note saved in the same folder.

   If the incident/concern pertains to the conduct of a member of staff, these should be referred to the head teacher and will be dealt with as necessary and stored within the administration network.

   Any low level correspondence i.e. queries, appointment arrangements etc. involving parents can be deleted once replied to. Please note that in the event of a parent requesting access to their data any emails regarding their child would need to be made available.

4. Photographs of pupils should only be taken on school devices.

5. Staff should not share log-in details or passwords for any service/server that contains pupil information i.e. DCPro, school reports, IEPs etc. Once staff members have finished using/are moving away from a computer where others can gain access the user should lock/log-off/minimise as appropriate.

6. Particular care should be taken to maintain the security of personal details recorded on care plans, medical permissions and emergency contacts during school visits.

7. In the event of a security breach i.e. loss of a memory stick, theft of device, pupils books stolen from a car, staff members should inform the Data Protection Officer/headteacher as soon as possible so that the security breach protocol can be started.

8. When a staff member ceases working at the school all emails, data and documents created during their period of employment, which contain personal data should be left at the school. Upon negotiation and where there are no data protection implications items may be copied for future use with other employers.

9. Staff should ensure a clear desk at the end of each working day.

Signed _____ Date _____